UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/745,260	12/20/2000	Peter Phaal	21906-702	8339

7590	10/26/2005

David G. Beck
Bingham McCutchen LLP
3 Enbarcadero Center
Suite 1800
San Fransico, CA 94111

EXAMINER
TSEGAYE, SABA

ART UNIT	PAPER NUMBER
2662	

DATE MAILED: 10/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

Response to Amendment

1.   This is a response to the amendment filed 07/22/05. Claims 1-5 and 7-45 are pending.

Currently no claims are in condition for allowance.

Claim Objections

2.   Claim 27 is objected to because of the following informalities: claim 27 is identical with

claim 22. Appropriate correction is required.

Claim Rejections - 35 USC § 102

3.   Claims 1-3, 5, 10-20, 22, 26-36 and 42-45 are rejected under 35 U.S.C. 102(e) as being

anticipated by Lyle (US 6,886,102).

Regarding claim 1, Lyle discloses a method of monitoring a network switch (108a-b)

having a plurality of regular ports (users are connected to switch 108a-b; see figure 1) between

which network traffic data packets are forwarded and an external mirror port (110a-b),

comprising:

        selecting at least one of said regular ports (column 7, lines 39-49)

        mirroring a data packet of the selected port to said external mirror port (the tracking

system computer 102 is connected to the respective copy port of switches 108a-b via the copy

port connection lines 110a-b) (column 5, lines 1-45);

        extracting the network address information of said mirrored data packet (column 10,

lines 1-34),

determining port information of said network address information in response to the

network address information extraction (column 10, lines 44-59) and

performing network analysis of said network switch (column 10, lines 44-59).

Regarding claims 14, 28 and 29, Lyle discloses, in Fig. 1, a method to monitor a network

switch (108), comprising:

obtaining at least a portion of data packets being handled by the network switch, wherein

each of the data packets comprises network address information (the sniffer module (102)

monitors switch and router ports to detect if a particular port is receiving an unusually high

number of data packets of any type with a certain target destination or recipient address (see

columns 5 and 10&) fig. 1 shows; monitoring network traffic through mirror port 112);

extracting the network address information from the data packets (capturing the network

traffic traveling between the network devices (column 5, lines 44-59); and

determining port information of the network address information in response to the

network address information extraction (the sniffer module (102) monitors switch and router

ports to detect if a particular port is receiving an unusually high number of data packets of any

type with a certain target destination or recipient address (see column 5, lines 44-59); and

performing network analysis of said network switch (statistical information from the

statistics database is used to determine if the rate of certain types of messages exceeds a normal

level).

Regarding claims 2, 15 and 30, Lyle discloses the method wherein the port information

comprises physical information (column 10, lines 44-59).

Regarding claims 3, 20 and 36, Lyle discloses the method wherein the port information

determination comprises interrogating the network switch to obtain the port information using

the network address information (column 10, lines 44-59).

Regarding claims 5, 22, 27 and 31, Lyle discloses the method wherein the network

address information extraction and the port information determination are performed in an

external monitor device (column 10, lines 44-59).

Regarding claims 10, 26 and 42, Lyle discloses the method further comprising

maintaining at least one lookup table correlating the network address information with the port

information (column 8, lines 45-51).

Regarding claims 11, 12, 17, 18, 33 and 34, Lyle discloses the method wherein the

network address information comprises a source address and a destination address of the

mirrored data packet (column 10, lines 44-59; column 13, lines 37-47).

Regarding claims 13 and 43, Lyle discloses the method wherein the network switch is a

routing switch (column 6, lines 37-51).

Regarding claims 16 and 32, Lyle discloses the method wherein the network switch

comprises a plurality of regular ports (users are connected to switch 108a-b; see figure 1) and a

mirror port (the tracking system computer 102 is connected to the respective copy port of

switches 108a-b via the copy port connection lines 110a-b), the mirror port being able to mirror

network traffic for at least one of the regular ports, wherein the portion of data packets are obtained from the mirror port (column 5, lines 1-17; column 10, lines 1-34).

Regarding claims 19 and 35, Lyle discloses the method wherein the network switch comprises a plurality of regular ports (users are connected to switch 108a-b; see figure 1), wherein the portion of data packets are obtained by passively tapping at least one of the regular ports (column 5, lines 1-17; column 10, lines 1-34).

Regarding claim 44, Lyle discloses the method further comprising associating the port information with information contained in the obtained portion of data packets (column 10, lines 16-34).

Regarding claim 45, Lyle discloses the method further comprising performing network analysis of the network switch using the port information and associated data packet information (column 10, lines 16-34).

4.   Claims 1-3, 5, 11-20, 22, 27-36 and 43-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Hegge et al. (US 2001/0055274), hereafter referred to Hegge.

Regarding claim 1, Hegge discloses a method of monitoring a network switch (10) having a plurality of regular ports (see ports 25 and 30 in figure 1) between which network traffic data packets are forwarded and an external mirror port (35), comprising:

selecting at least one of said regular ports (25);

mirroring a data packet of the selected port to said external mirror port (35) (see

paragraph 0014);

extracting the network address information of said mirrored data packet (data flows are

identified and copied to an appropriate mirror port in response to the type of flow and a monitor

device monitors specific types of traffic);

determining port information of said network address information in response to the

network address information extraction (0017; 0021); and

performing network analysis of said network switch (a monitor device monitors specific

types of traffic; 0027).

Regarding claims 2 and 15, Hegge discloses that said port information refers to physical

information (see figure 1 and (0017)).

Regarding claim 3, Hegge discloses that said port information determination comprises

interrogating said switch to obtain said port information using said network address information

(determining whether the information is a part of particular flow of information that is a member

of pre-selected group of flows of information ; 0017).

Regarding claim 5, Hegge disclose the method wherein the network address information

extraction and the port information determination are performed in an external monitor device

(40; 0014).

Regarding claims 11 and 12, Hegge discloses that said network address information

comprises source address and the destination address of said mirrored data packet (packets that

have been transmitted using the TCP/IP protocol and it is part of this standard to have the source

and destination addresses of the packet included in each packet to allow for proper routing, thus

the packets received by the test equipment have the source and destination addresses of where

that packet came from and where they are going to (see 0021 and 0028)).

Regarding claims 13 and 43, Hegge discloses that said network switch is a routing switch

(the switch routs packets over a switches network (see figure 1; 0016)).

Regarding claims 14 and 28, Hegge discloses a method to monitor a network switch,

comprising:

externally obtaining at least a portion of data packets received at the network switch (10),

wherein each of the data packets comprises network address information (the processor 15

identifies data flows, i.e., type of traffic, and switches packets to appropriate queues 20

according to flow and destination; monitoring network traffic through mirror port 35);

extracting the network address information from the obtained portion of data packets

(data flows are identified and copied to an appropriate mirror port in response to the type of flow

and a monitor device monitors specific types of traffic); and

determining port information of the network address information in response to the

network address information extraction (0017); and

performing network analysis of said network switch (a monitor device monitors specific

types of traffic; 0027).

Regarding claims 16 and 32, Hegge discloses that said network switch having a plurality

of regular ports (25, 30) and a mirror port (35), said mirror port being able to mirror network

traffic for at least one of said regular ports, wherein said portion of data packets are obtained

from said mirror port (the switch and the test equipment are coupled to each other (see figure 1;

and 0014).

Regarding claims 17, 18, 33 and 34, Hegge discloses that said network address

information comprises source address and the destination address of said mirrored data packet

(packets that have been transmitted using the TCP/IP protocol and it is part of this standard to

have the source and destination addresses of the packet included in each packet to allow for

proper routing, thus the packets received by the test equipment have the source and destination

addresses of where that packet came from and where they are going to (see 0021 and 0028)).

Regarding claims 19 and 35, Hegge discloses the method wherein the network switch

comprises a plurality of regular ports (25), wherein said portion of data packets are forwarded to

said monitor device (40) by passively tapping at least one of said regular ports (data traffic

through the switch to other ports is copied to the mirror port for monitoring by the IDS and the

IDS itself communicates to other devices attached to the switch, for example a console, using the

mirror port).

Regarding claims 20 and 36, Hegge discloses that said determining step comprising: interrogating said switch to obtain said port information using said network address information (determining whether the information is a part of particular flow of information that is a member of pre-selected group of flows of information).

Regarding claims 22 and 27, Hegge disclose the method wherein the network address information extraction and the port information determination are performed in an external monitor device (40; 0014).

Regarding claim 29-31 Hegge discloses that said port information refers to physical information of said network address information in said network switch (the port number corresponds to the physical port that the network node is attached to (see figure 1)).

Regarding claim 44, Hegge discloses the method further comprising associating the port information with information contained in the data packets ((fig.1, when traffic captured that traveled between the network devices, it is inherent to determine port information in order to forward the data packet to the destination).

Regarding claim 45, Hegge discloses the method, further comprising performing network analysis of said network switch using said port information and associated data packet information (data traffic through the switch to other ports is copied to the mirror port for

monitoring by the IDS and the IDS itself communicates to other devices attached to the switch,

for example a console, using the mirror port).

5.   Claims 14-20, 22, 26-36 and 42-45 are rejected under 35 U.S.C. 102(b) as being

anticipated by Pendleton et al. (USPN 5,982,753), hereafter referred to as Pendleton.

Regarding claims 14 and 28, Pendleton discloses a method to monitor a network switch,

comprising:

obtaining at least a portion of data packets being handled by the network switch, wherein

each of the data packets comprises network address information (the test equipment uses passive

monitoring to receive packets that are transported between network nodes (see columns 5 and

7&) fig. 1 shows; monitoring network traffic through mirror port 12);

extracting the network address information from the data packets (capturing the network

traffic traveling between the network devices (column 5, lines 19-23 &); test equipment uses

passive monitoring to perform a discovery process which allows the test equipment to extract

MAC and/or IP address from the passively monitored packets (see figure 6 and columns 5 and

7)); and

determining port information of the network address information in response to the

network address information extraction (when traffic captured that traveled between the network

devices, it is inherent to determine port information in order to forward the data packet to the

destination (see column 5, lines19-23); further the test equipment uses MIBs to build a port table

(see item 47 in figure 5)); and

performing network analysis of said network switch (the test equipment analyzes reports

regarding the ports and related traffic through the switch (see column 8; column 5, lines 19-27)).

Regarding claim 15, Pendleton discloses that said port information refers to physical

information of said network address information in said network switch (the port number

corresponds to the physical port that the network node is attached to (see figures 2 and 3)).

Regarding claim 16, Pendleton discloses that said network switch having a plurality of

regular ports and a mirror port (see ports 11,16,20 and 22 in figures 1 and 2), said mirror port

being able to mirror network traffic for at least one of said regular ports (the test instrument can

passively receive traffic that it transported between network nodes (see figures 1-3 and column

5)), wherein said portion of data packets are obtained from said mirror port (the switch and the

test equipment are coupled to each other (see figures 1 and 2)).

Regarding claims 17, 18, 33 and 34, Pendleton discloses that said network address

information comprises source address and the destination address of said data packet (the passive

discovery process includes the test equipment receiving IP packets that have been transmitted

using the TCP/IP protocol and it is part of this standard to have the source and destination

addresses of the packet included in each packet to allow for proper routing, thus the packets

received by the test equipment have the source and destination addresses of where that packet

came from and where they are going to (see columns 5-7)).

Regarding claim 19, Pendleton discloses that said network switch comprising a plurality of regular ports (the switch has a plurality of ports (see figures 1-3)), wherein said data packets are forwarded to said monitor device by passively tapping at least one of said regular ports (the test equipment passively taps into the switch (see figures 1-3 and columns 5 and 7)).

Regarding claim 20, Pendleton discloses that said determining step comprising: interrogating said switch to obtain said port information using said network address information (the switches MIBs can also be requested in order to build the port table (see column 7 and figure 5)).

Regarding claim 22, Pendleton discloses that said first request and said second request are SNMP requests (the test equipment requests the Mms from the switch uses SNMP queries (see column 5)).

Regarding claims 26 and 42, Pendleton discloses maintaining at least one lookup table correlating said network address information with said port information (a port table is maintained (see item 47 in figure 5)).

Regarding claims 27 and 43, Pendleton discloses that said network switch is a routing switch (the switch routs packets over a switches network (see figures 1-3)).

Regarding claim 29-31 Pendleton discloses that said port information refers to physical

information of said network address information in said network switch (the port number

corresponds to the physical port that the network node is attached to (see figures 2 and 3)).

Regarding claim 32, Pendleton discloses the method that said network switch having a

plurality of regular ports (see Figs. 1-3) and a mirror port (11, 12), said mirror port being able to

mirror network traffic for at least one of the regular ports, wherein said portion of data packets

are obtained from said mirror port (the test equipment uses passive monitoring to receive packets

that are transported between network nodes (see columns 5 and 7)).

Regarding claim 35, Pendleton discloses the method that said network switch comprising

a plurality of regular ports 9see figures 1-3), wherein said data packets are obtained by passively

tapping at least one of said regular ports (the test equipment uses passive monitoring to receive

packets that are transported between network nodes (see columns 5 and 7)).

Regarding claim 36, Pendleton discloses that said port information determination

comprises interrogating said switch to obtain said port information using said network address

information (the switches MIBs can also be requested in order to build the port table (see column

7 and figure 5)).

Regarding claim 44, Pendleton discloses the method further comprising associating the

port information with information contained in the data packets ((fig.1, when traffic captured that

traveled between the network devices, it is inherent to determine port information in order to forward the data packet to the destination); further the test equipment uses MIBs to build a port table (see item 47 in figure 5)).

Regarding claim 45, Pendleton discloses the method, further comprising performing network analysis of said network switch using said port information and associated data packet information (the test equipment uses passive monitoring to receive packets that are transported between network nodes (see columns 5 and 7)).

Allowable Subject Matter

6.   Claims 4, 7-9, 21, 23-25 and 37-41 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Response to Arguments

7.   Applicant's arguments with respect to claims 1-5 and 7-45 have been considered but are moot in view of the new ground(s) of rejection.
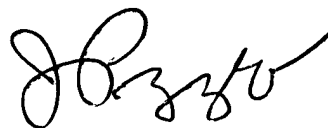
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saba Tsegaye whose telephone number is (571) 272-3091. The examiner can normally be reached on Monday-Friday (7:30-5:00), First Friday off.

    If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Hassan Kizou can be reached on (571) 272-3088. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

    Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ST
October 17, 2005

JOHN PEZZLO
PRIMARY EXAMINER